

INTERSECTIVE S_n POLYNOMIALS WITH FEW IRREDUCIBLE FACTORS

DANIELA BUBBOLONI AND JACK SONN

ABSTRACT. An intersective polynomial is a monic polynomial in one variable with rational integer coefficients, with no rational root and having a root modulo m for all positive integers m . Let G be a finite noncyclic group and let $r(G)$ be the smallest number of irreducible factors of an intersective polynomial with Galois group G over \mathbb{Q} . Let $s(G)$ be smallest number of proper subgroups of G having the property that the union of their conjugates is G and the intersection of all their conjugates is trivial. It is known that $s(G) \leq r(G)$. It is also known that if G is realizable as a Galois group over the rationals, then it is also realizable as the Galois group of an intersective polynomial. However it is not known, in general, whether there exists such a polynomial which is a product of the smallest feasible number $s(G)$ of irreducible factors. In this paper, we study the case $G = S_n$, the symmetric group on n letters. We prove that for every n , either $r(S_n) = s(S_n)$ or $r(S_n) = s(S_n) + 1$ and that the optimal value $s(S_n)$ is indeed attained for all odd n and for some even n . Moreover, we compute $r(S_n)$ when n is the product of at most two odd primes and we give general upper and lower bounds for $r(S_n)$.

1. INTRODUCTION

An *intersective* polynomial is a monic polynomial in one variable with rational integer coefficients, with no rational root and having a root modulo m for all positive integers m , or equivalently, having a root in \mathbb{Q}_p for all (finite) p . Let G be a finite noncyclic group and let $r(G)$ be the smallest number of irreducible factors of an intersective polynomial with Galois group G over \mathbb{Q} . There is a group-theoretically defined lower bound for $r(G)$, given by the smallest number $s(G)$ of proper subgroups of G having the property that the union of the conjugates of those subgroups is G and their intersection is trivial. This follows from

Proposition 1.1. ([11, Prop. 2.1]) *Let K/\mathbb{Q} be a finite Galois extension with Galois group G . The following are equivalent:*

Date: July 31, 2015.

2000 Mathematics Subject Classification. Primary 11R32; Galois theory.

Key words and phrases. symmetric group, Galois group, decomposition group.

(1) K is the splitting field of a product $f = g_1 \cdots g_m$ of m irreducible polynomials of degree greater than 1 in $\mathbb{Q}[x]$ and f has a root in \mathbb{Q}_p for all (finite) primes p .

(2) G is the union of the conjugates of m proper subgroups A_1, \dots, A_m , the intersection of all these conjugates is trivial, and for all (finite) primes \mathfrak{p} of K , the decomposition group $G(\mathfrak{p})$ is contained in a conjugate of some A_i .

Recall that the decomposition group $G(\mathfrak{p})$ is the stabilizer in G of the prime \mathfrak{p} . Note also that we have $2 \leq s(G) \leq r(G)$, the first inequality holding because no group is the union of the conjugates of a single proper subgroup. The second inequality holds by definition.

It is natural to ask for which G , realizable over \mathbb{Q} , is $s(G) = r(G)$? This paper focuses on this question for the symmetric groups $G = S_n$ of degree $n \geq 3$, which are well known to be realizable over \mathbb{Q} . We view S_n as naturally acting on the set $\Omega = \{1, \dots, n\}$.

If we drop the trivial intersection condition in the definition of $s(G)$, we obtain the *normal covering number* of G , denoted by $\gamma(G)$ in the group theory literature. We recall some terminology from [2]. If H_1, \dots, H_l , with $l \in \mathbb{N}$, are pairwise non-conjugate proper subgroups of G such that $G = \bigcup_{g \in G} \bigcup_{i=1}^l H_i^g$, we say that $\Delta = \{H_i^g \mid 1 \leq i \leq l, g \in G\}$ is a *normal covering* of G and that $\delta = \{H_1, \dots, H_l\}$ is a *basic set* for G generating Δ . We call the elements of Δ the *components* and the elements of δ the *basic components* of the normal covering Δ . The minimum cardinality $\gamma(G)$ of a basic set is called the normal covering number of G . Recall that $\gamma(G) \geq 2$ and note that $\gamma(G)$ can be seen as the minimum number of proper subgroups of G such that every cyclic subgroup of G lies in some conjugate of one of them. By definition, we have $\gamma(G) \leq s(G)$. On the other hand, if the trivial intersection condition does not hold for a set of subgroups whose conjugates cover G , adding the trivial subgroup restores the trivial intersection property and thus, for every finite group G , we have $s(G) \in \{\gamma(G), \gamma(G) + 1\}$. In particular, for the symmetric groups, it is easily seen that $s(S_n) = \gamma(S_n)$ (Lemma 2.1). We then accordingly ask whether, for every $n \geq 3$, $\gamma(S_n) = r(S_n)$.

Fortunately, much is already known about $\gamma(S_n)$. In [4, Theorem 1.1], it is proved that γ grows linearly with n , in the sense that there exists $k \in \mathbb{R}$, with $0 < k \leq 2/3$, such that

$$(1.1) \quad kn \leq \gamma(S_n) \leq 2n/3$$

for all $n \geq 3$. In [2] exact values of $\gamma(S_n)$ are given for all n odd and divisible by at most two distinct primes. It has been shown for the case $\gamma(S_n) = 2$, which holds exactly for $3 \leq n \leq 6$, that there exist Galois realizations for which $r(S_n) = 2$ [10]. The present paper gives for the first time an infinite set of n for which $r(S_n) = \gamma(S_n)$. In fact, we show that this holds for all odd n (Proposition 5.1).

To state our first main result, we need to introduce a class of metacyclic subgroups of S_n , which are in fact abelian on two generators. For $m \in \mathbb{N}$, denote by

C_m the cyclic group of order m . Let M be a subgroup of S_n of the form $C_{2m} \times C_2$, for some $m \in \mathbb{N}$, with C_2 generated by a transposition $\tau = (i\ j)$. We call M a *special metacyclic* subgroup of S_n and denote by $\mathcal{M}(S_n)$ the set of special metacyclic subgroups of S_n . We claim that the factor C_{2m} in $M \in \mathcal{M}(S_n)$ can be chosen generated by $\sigma \in S_n$ such that $\sigma(i) = i$ and $\sigma(j) = j$. Indeed, let $C_{2m} = \langle \psi \rangle$, $C_2 = \langle \tau \rangle$ and $M = \langle \psi \rangle \times \langle \tau \rangle$. Note that $|M| = 4m$. Then $C_{2m} = \langle \psi \rangle$ is contained in the centralizer of τ in S_n , which is the direct product of $\langle \tau \rangle$ and the subgroup U of S_n fixing i and j . In particular, we have $\psi = \sigma$ or $\psi = \sigma\tau$, for some $\sigma \in U$. In the first case our claim is obvious. In the second case, we have $M = \langle \sigma\tau \rangle \times \langle \tau \rangle = \langle \sigma \rangle \times \langle \tau \rangle$ and $4m = 2|\sigma|$ gives $|\sigma| = 2m$, so that σ generates a cyclic group of order $2m$. Throughout the paper the two generator σ and τ of M will be always chosen such that $\tau = (i\ j)$, $\sigma(i) = i$ and $\sigma(j) = j$.

Theorem A. *For any n , the symmetric group S_n is realizable infinitely often as a Galois group over \mathbb{Q} , with all decomposition groups either cyclic or special metacyclic of the form $C_{2m} \times C_2$, where the factor C_2 generated by a transposition is the inertia group. The factor C_{2m} can be chosen so that it fixes the two letters moved by the transposition.*

Theorem A suggests the definition of a further useful parameter $\gamma'(S_n)$. We call a basic set δ' *special* if every subgroup of S_n which is either cyclic or special metacyclic, is contained in a conjugate of a component in δ' . If $\delta' = \{H_1, \dots, H_l\}$ is a special basic set, we call the corresponding covering $\Delta' = \{H_i^g \mid 1 \leq i \leq l, g \in S_n\}$ a *special normal covering* of S_n . The minimum cardinality of a special basic set for G is called the *special normal covering number* of S_n and denoted by $\gamma'(S_n)$; a special basic set of size $\gamma'(S_n)$ is called a *minimal special basic set*. Note that if $n = 3$, no special metacyclic subgroup exists and thus, $\gamma'(S_3) = \gamma(S_3) = 2$.

For $x \in \mathbb{N}$, with $1 \leq x \leq n/2$, consider the intransitive subgroup of S_n , defined by $P_x = \{\psi \in S_n : \psi(\{1, \dots, x\}) = \{1, \dots, x\}\}$. Clearly, if $X \subseteq \Omega$ has size $c \in \mathbb{N}$, for some $c < n$, and $G = \{\psi \in S_n : \psi(X) = X\}$, then there exists $g \in S_n$ such that $G = P_x^g$, where $x = \min\{c, n - c\}$. Moreover, the set of maximal subgroups of S_n which are intransitive is given by the conjugates of the subgroups in \mathcal{P} , where

$$(1.2) \quad \mathcal{P} = \{ P_x : 1 \leq x < n/2 \}.$$

Recall that, for n even, the intransitive subgroup $P_{n/2}$ is not maximal in S_n because it is properly contained in the maximal imprimitive subgroup $S_{n/2} \wr S_2$ (see Section 4).

Consider $M \in \mathcal{M}(S_n)$, with generators σ and $\tau = (i\ j)$, so that $\sigma(i) = i$ and $\sigma(j) = j$. Then, for $X = \{i, j\}$, we have $\psi(X) = X$ for all $\psi \in M$ and so, up to conjugacy, M is contained in P_2 . It follows that $\gamma(S_n) \leq \gamma'(S_n) \leq \gamma(S_n) + 1$, and $\gamma'(S_n) = \gamma(S_n)$ if there exists a minimal normal covering of S_n admitting as component P_2 or some proper overgroup H of P_2 . Note that, P_2 being maximal in S_n for $n \geq 5$, this last possibility can happen only for $n = 4$, through $H = S_2 \wr S_2$.

Interestingly, there are examples of n for which $\gamma'(S_n) = \gamma(S_n)$ even though no minimal normal covering of S_n has a component containing P_2 (Proposition 5.13).

Combining Proposition 1.1 with Theorem A, we easily obtain the following interesting corollary.

Corollary B. *Let $n \in \mathbb{N}, n \geq 3$. Then $2 \leq \gamma(S_n) \leq r(S_n) \leq \gamma'(S_n)$. In particular, $r(S_n)$ equals $\gamma(S_n)$ or $\gamma(S_n) + 1$, and equals $\gamma(S_n)$ if there exists a minimal normal covering of S_n which includes P_2 .*

Theorem A and Corollary B naturally raise two questions.

Arithmetic Question. *Is S_n realizable over the rationals \mathbb{Q} with all decomposition groups cyclic?*

The answer to this question appears to be unknown. When the answer is yes for a given n , it is immediate also that $r(S_n) = \gamma(S_n)$.

Group-theoretic Question 1. *Is $\gamma'(S_n) = \gamma(S_n)$ for all $n \in \mathbb{N}, n \geq 3$?*

An affirmative answer to this question also gives $r(S_n) = \gamma(S_n)$. In Section 5, we give an affirmative answer for n odd (Proposition 5.1) but the question remains open, in general, for n even. An indication of the complexity for the even case is illustrated by the cases $n = 10$ and $n = 14$, which we treat in Section 5.3. Some support for an affirmative answer in the general case might be given by the fact that any known upper bound for $\gamma(S_n)$ holds also for $\gamma'(S_n)$ (Propositions 5.8 and 5.16). Moreover, for all the n such that the value of $\gamma(S_n)$ is known, we have $\gamma'(S_n) = \gamma(S_n)$.

We conclude the paper by finding for $r(S_n)$ as well as for $\gamma'(S_n)$ the same linear bounds (1.1) known for $\gamma(S_n)$ (Proposition 6.1).

2. INTERSECTIVE S_n POLYNOMIALS WITH FEW IRREDUCIBLE FACTORS

We start by noting that for the symmetric group, the parameters s and γ coincide:

Lemma 2.1. *If $\delta = \{H_1, \dots, H_k\}$ is a basic set for S_n , then $\bigcap_{\sigma \in S_n} \bigcap_{i=1}^k H_i^\sigma = 1$. In particular $\gamma(S_n) = s(S_n)$.*

Proof. Assume that $K = \bigcap_{\sigma \in S_n} \bigcap_{i=1}^k H_i^\sigma \neq 1$. Since $K \triangleleft S_n$, the only possibility is $K = A_n$. Then, for every $i \in \{1, \dots, k\}$, we have $A_n \leq H_i < S_n$, which gives $H_i = A_n$ and thus $\delta = \{A_n\}$, a contradiction. Next let δ be a minimal basic set with $\gamma(S_n)$ components. By what is shown above, δ realises the trivial intersection property, thus $s(S_n) \leq \gamma(S_n)$. As $s(G) \geq \gamma(G)$ for all finite groups G , the equality $\gamma(S_n) = s(S_n)$ holds. \square

The proof of Theorem A is based on a construction of Kedlaya ([7]) of infinitely many Galois realizations of the symmetric groups S_n over \mathbb{Q} with squarefree discriminants, together with an earlier result of Kondo ([8]).

Theorem 2.2. (Kedlaya) *Let $n > 1$ be an integer and let S be a finite set of primes. Then there exist infinitely many monic irreducible polynomials $P(x)$ of degree n , with integer coefficients, such that the discriminant of $P(x)$ is squarefree and not divisible by any of the primes in S .*

Proof of Theorem A. Let $n \in \mathbb{N}, n \geq 3$ and $S = \{p \text{ prime} : p \leq n\}$. Let $P(x)$ be a polynomial given by Theorem 2.2 and let K be its splitting field. Since, as pointed out by Kedlaya in [7], citing Kondo [8], an irreducible polynomial of degree n with rational integer coefficients whose discriminant is squarefree has Galois group S_n over \mathbb{Q} , we have that $G(K/\mathbb{Q}) = S_n$. Let p be a rational prime. If p is unramified in K , then its decomposition group is cyclic. We may therefore assume p is ramified in K . By Kondo [8, Lemma 2, Theorem 2], the inertia group of a prime \mathfrak{p} of K dividing p is of order two and generated by a transposition τ . As p divides the discriminant of $P(x)$, we have that $p > n$. In particular, p does not divide $n! = |S_n|$. Since the ramification index e_p divides the order of the Galois group of K/\mathbb{Q} , p does not divide e_p , so that p is tamely ramified in K . Recall now that, for any prime, the inertia group is a normal subgroup of the decomposition group, and the quotient group is cyclic of order f , where f is the inertia degree of the prime \mathfrak{p} over p . For a tamely ramified prime, the inertia group is cyclic as well, and if it is also of order 2 as in our case, it is central. Thus the decomposition group is metacyclic abelian. Moreover, as τ is not a square in S_n , the decomposition group splits into a direct product of $\langle \tau \rangle$ and a cyclic group $C = \langle \sigma \rangle$ of order f . If f is odd, then the decomposition group is cyclic. If f is even, then the decomposition group belongs to $\mathcal{M}(S_n)$ and the possibility to choose the factor C fixing the two letters moved by τ is guaranteed by the discussion about the groups in $\mathcal{M}(S_n)$ made in the introduction. \square

Proof of Corollary B. The inequality $\gamma(S_n) \leq r(S_n)$ follows from Lemma 2.1 recalling that, by Proposition 1.1, $s(S_n) \leq r(S_n)$. To show $r(S_n) \leq \gamma'(S_n)$, let δ' be a special basic set of S_n of minimal cardinality $\gamma'(S_n)$. By Theorem A, there exists an S_n -extension K of \mathbb{Q} with decomposition groups normally covered by δ' . By Proposition 1.1, there exists an intersective polynomial with splitting field K which is a product of $\gamma'(S_n)$ irreducible factors. Hence $r(S_n) \leq \gamma'(S_n)$. The final assertion is immediate from the first, together with the relation between $\gamma(S_n)$ and $\gamma'(S_n)$ discussed in the introduction. \square

3. PARTITIONS AND PERMUTATIONS

The next sections of the paper deal with the question of whether or not $\gamma'(S_n) = \gamma(S_n)$. To start with we need some definitions.

3.1. Partitions and cuts. Let $n, k \in \mathbb{N}$, with $k \leq n$. A k -partition of n is an unordered k -tuple $T = [x_1, \dots, x_k]$, with $x_i \in \mathbb{N}$ for all $i \in \{1, \dots, k\}$, such that $n = \sum_{i=1}^k x_i$. The x_i are called the *terms* of the k -partition and, obviously, we have $1 \leq x_i \leq n$. If T is a k -partition of n , for some $k \in \mathbb{N}$, we say that T is a partition of n . We denote by $\mathcal{T}(n)$ the set of partitions of n . Fix $v \geq n$ and call v the representation length for $\mathcal{T}(n)$. If $T \in \mathcal{T}(n)$, let $m_j \in \{0, 1, \dots, n\}$ be the number of times in which $j \in \{1, \dots, v\}$ appears as a term in T . We call m_j the *multiplicity* of j in T and say that $T = [1^{m_1}, 2^{m_2}, \dots, v^{m_v}]$ is the representation of T of length v . Note that, within this representation, we have $\sum_{j=1}^v j m_j = n$ and that the exponents m_j do not represent a power. Obviously, $m_j = 0$ for all $n < j \leq v$. The multiplicities equal to 1 are usually omitted. In many contexts also the multiplicities equal to 0 are omitted, but in others some of them can be usefully put in evidence. Let $T = [1^{m_1}, 2^{m_2}, \dots, n^{m_n}] \in \mathcal{T}(n)$ be represented with length n . Let, for every $j \in \{1, \dots, n\}$, $0 \leq s_j \leq m_j$ be such that $c = \sum_{j=1}^n j s_j$ satisfies $0 < c < n$. Then $T' = [1^{s_1}, 2^{s_2}, \dots, n^{s_n}] \in \mathcal{T}(c)$ is called a *subpartition* of T . Note that T' is also represented with length n . Let now $c \in \mathbb{N}$, with $0 < c < n$ and use n as a common representation length for $\mathcal{T}(n)$, $\mathcal{T}(c)$ and $\mathcal{T}(n-c)$. If $T_1 \in \mathcal{T}(c)$ is a subpartition of T , then T_1 defines, in a natural way, the *complementary partition* $T_2 = [1^{m_1-s_1}, 2^{m_2-s_2}, \dots, n^{m_n-s_n}] \in \mathcal{T}(n-c)$. We say that (T_1, T_2) realizes a c -cut for T and write $T = [T_1 \mid T_2]$. If $T = [T_1 \mid T_2]$ is a cut for T , we say that the cut *isolates* T' if T' is a subpartition of T_1 or T_2 . Note that if the c -cut $[T_1 \mid T_2]$ isolates T' , then also the $(n-c)$ -cut $[T_2 \mid T_1]$ isolates T' .

For instance, if $T = [1^3, 2^2, 5]$, $n = 12$, $c = 7$ and $T_1 = [1^2, 5]$, then T_1 is a partition of 7 which is a subpartition of T , and $T_2 = [1, 2^2]$ is the complementary partition of $n - c = 5$. Thus $T = [1^2, 5 \mid 1, 2^2]$ is a 7-cut for T , which isolates $T' = [1, 5]$ as well as $T' = [2^2]$ but not $T' = [2, 5]$.

3.2. The type of a permutation. Let $\sigma \in S_n$ and let $\mathcal{O}(\sigma)$ be the set of orbits of σ in the natural action on Ω . Let X_1, \dots, X_k be the distinct elements of $\mathcal{O}(\sigma)$ and put $x_i = |X_i|$. Then the unordered list $T_\sigma = [x_1, \dots, x_k]$ is a k -partition of n , called the *type* of σ . Note that the fixed points of σ correspond to the $x_i = 1$, while the lengths of the disjoint cycles in which σ splits are given by the $x_i \geq 2$. Recall that the order $|\sigma|$ of σ may be recovered by T_σ through $|\sigma| = \text{lcm}\{x_i\}_{i=1}^k$. In particular, if $|\sigma|$ is even, then at least one x_i is even. Clearly, for all $k \in \mathbb{N}$, with $1 \leq k \leq n$, each k -partition of n is the type of some permutation in S_n . Therefore $\mathcal{T}(n)$ coincides with the set of types for S_n . The concept of type is crucial in dealing with normal coverings for the symmetric group, because $\sigma, \nu \in S_n$ are conjugate in S_n if and only if $T_\sigma = T_\nu$. Thus $\delta = \{H_1, \dots, H_l\}$ is a basic set for S_n

if and only if for every $T \in \mathcal{T}(n)$ there exists $j \in \{1, \dots, l\}$ such that H_j contains a permutation σ with $T_\sigma = T$. When a subgroup H of S_n contains a permutation of type T we say that ‘ T belongs to H ’ and we write $T \in H$.

3.2.1. The canonical form of T_σ . Let $M \in \mathcal{M}(S_n)$ with generators σ and τ . Recall that $\tau = (i \ j)$ is a transposition while σ is a permutation with $|\sigma|$ even, $\sigma(i) = i$ and $\sigma(j) = j$. In particular, $T_\tau = [1^{n-2}, 2]$ and $T_\sigma = [1^2, x_1, \dots, x_k]$, where $k = |\mathcal{O}(\sigma)| - 2 \geq 1$. Note that $1 \leq x_i < n$, for all $1 \leq i \leq k$. We say that the type of σ is represented in canonical form if $x_1, \dots, x_k \in \mathbb{N}$ are arranged so that there exists $s \in \mathbb{N}$, with $s \leq k$ such that x_i is even for $1 \leq i \leq s$, while x_i is odd for $s < i \leq k$. We set $m = k - s \geq 0$. Then, $m = 0$ means that the terms x_i in T_σ are even for all $1 \leq i \leq k$.

4. MAXIMAL SUBGROUPS OF S_n

In order to determine $\gamma(S_n)$ or $\gamma'(S_n)$, we may obviously assume that the components of a normal covering are maximal subgroups of S_n . These subgroups may be intransitive, primitive or imprimitive. The intransitive ones have been described in the introduction as the conjugates of the subgroups in \mathcal{P} , with \mathcal{P} defined in (1.2).

Let $n = bm$, where $b \mid n$ and $2 \leq b \leq n/2$. If \mathcal{B} is a partition of Ω into m subsets of size b , we say that \mathcal{B} is a (b, m) -block system for Ω . The imprimitive maximal subgroups of S_n are the stabilisers of all the possible block systems. Consider, for $j \in \{0, \dots, m-1\}$, the m proper subsets of Ω of size b given by $B_j = \{jb + i : i \in \{1, \dots, b\}\}$. Then $\mathcal{B}_0 = \{B_j : j \in \{0, \dots, m-1\}\}$ is a particular (b, m) -block system for Ω and we denote by $S_b \wr S_m$ its stabiliser in S_n . Then the set of imprimitive maximal subgroups of S_n is obtained by the conjugates of the subgroups in the set \mathcal{W} , where

$$\mathcal{W} = \{ S_b \wr S_m : 2 \leq b \leq n/2, b \mid n, m = n/b \}.$$

The primitive maximal subgroups of S_n , different from A_n , do not play a significant role in the normal coverings and they are excluded in all the known minimal normal coverings, with the exception of the case n prime. Namely, for any prime $p \geq 5$, the group S_p admits a unique minimal normal covering generated by the basic set

$$\delta = \{ AGL_1(p) \cong C_p \rtimes C_{p-1}, P_k : 2 \leq k \leq \frac{p-1}{2} \},$$

admitting the primitive maximal component $AGL_1(p)$. In particular $\gamma(S_p) = \frac{p-1}{2}$ ([2, Proposition 7.1]). Recall also that the unique minimal normal covering of S_3 is generated by the basic set $\{A_3, P_1\}$. Since we have observed that $\gamma'(S_3) = \gamma(S_3)$, by Corollary B, we get

$$(4.1) \quad \gamma'(S_3) = \gamma(S_3) = r(S_3) = 2.$$

5. SPECIAL NORMAL COVERINGS AND NORMAL COVERINGS

In this section, we study Group-theoretic Question 1 exploring the link between $\gamma'(S_n)$ and $\gamma(S_n)$ for $n \in A$, where $A = \{n \in \mathbb{N} : n \geq 4\}$. We start by giving an affirmative answer in the case n odd and go on, in the general case, showing that all the known upper bounds for $\gamma(S_n)$ hold also for $\gamma'(S_n)$.

5.1. The odd degree case.

Proposition 5.1. *Let $n \in A$ be odd. Then every minimal basic set with maximal components contains P_2 . In particular, $\gamma'(S_n) = \gamma(S_n) = r(S_n)$.*

Proof. Let $n \geq 5$ be odd and δ be a basic set for S_n , with maximal components. Consider the type $T = [2, n-2]$. Since $\gcd(2, n) = 1$, by Lemma 5.2 in [2], the only maximal subgroup of S_n containing a permutation of type T is P_2 . It follows that $P_2 \in \delta$ and we conclude applying Corollary B. \square

5.2. The main bound g .

Definition 5.2. For $n \in A$, let $\nu(n)$ be the number of the distinct prime factors of n and write

$$(5.1) \quad n = p_1^{\alpha_1} \cdots p_{\nu(n)}^{\alpha_{\nu(n)}}$$

where, for every $i, j \in \{1, \dots, \nu(n)\}$, $\alpha_i \in \mathbb{N}$, p_i is a prime number and $p_i < p_j$, for $i < j$.

Define the function $g : A \rightarrow \mathbb{N}$ by

$$(5.2) \quad g(n) = \begin{cases} \frac{n}{2}(1 - \frac{1}{p_1}) & \text{if } \nu(n) = 1, \alpha_1 = 1 \\ \frac{n}{2}(1 - \frac{1}{p_1}) + 1 & \text{if } \nu(n) = 1, \alpha_1 \geq 2 \\ \frac{n}{2}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) + 1 & \text{if } \nu(n) = 2, (\alpha_1, \alpha_2) = (1, 1) \\ \frac{n}{2}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) + 2 & \text{otherwise} \end{cases}$$

Note that, in the cases with $\nu(n) = 1$, $\frac{n}{2}(1 - \frac{1}{p_1})$ counts the natural numbers less than $n/2$ and not divisible by p_1 ; in the cases with $\nu(n) \geq 2$, $\frac{n}{2}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$ counts the natural numbers less than $n/2$ and not divisible by either p_1 or p_2 ([5, Proposition 2.4]). Moreover, for every $n \in A$, $g(n) \geq 2$. The function g plays an important role in bounding $\gamma(S_n)$. When $\nu(n)$ is small and n is odd, then $g(n)$ gives the exact value for $\gamma(S_n)$. Namely, by [5, Proposition 3.1] and [2, Propositions 7.1, 7.5, 7.6] we have the following.

Proposition 5.3. *Let $n \in A$. Then:*

- i) $\gamma(S_n) \leq g(n)$, with equality when n is odd and $\nu(n) \leq 2$;

ii) if $\nu(n) = 2$ and $(\alpha_1, \alpha_2) \neq (1, 1)$ or if $\nu(n) \geq 3$, then

$$(5.3) \quad \delta_C = \{P_x : 1 \leq x < n/2, \gcd(x, p_1 p_2) = 1\} \cup \{S_{p_1} \wr S_{n/p_1}, S_{p_2} \wr S_{n/p_2}\}$$

is a basic set of order $g(n)$, called the canonical basic set.

There are other odd degree cases for which $\gamma(S_n) = g(n)$; for instance, by [5, Theorem 1.1], for $n = 15q$, that holds when q is an odd prime such that $q \equiv 2 \pmod{15}$ and $q \not\equiv 12 \pmod{13}$. Also, for all the even cases in which $\gamma(S_n)$ is known, we have $\gamma(S_n) = g(n)$; for instance, that holds for all even n , with $4 \leq n \leq 12$ (see [5, Table 1]). On the other hand, we stress that no general exact formula is known for $\gamma(S_n)$, when n is even, with a lack of knowledge even when n is a power of 2 (see [5, Problems 2 and 3]). The bound $\gamma(S_n) \leq g(n)$ is the best information we have on the number $\gamma(S_n)$, when n is even (see also Sections 5.4 and 5.5).

We now want to obtain the same inequality of Proposition 5.3 for $\gamma'(S_n)$. To that purpose, we need some preliminary results.

Lemma 5.4. *Let $n \in \mathbb{N}$ and $b, m \in \mathbb{N}$ with $b, m \geq 2$ such that $n = bm$. Let $l \in \mathbb{N}$ and, for $i \in \{1, \dots, l\}$, let $\sigma_i \in S_n$ be cycles with lengths divisible by b . If the σ_i are disjoint, then $\langle \sigma_1, \dots, \sigma_l \rangle$ is contained in a conjugate of $S_b \wr S_m$.*

Proof. By hypothesis, the length of σ_i is of the form $m_i b$, for some $m_i \in \mathbb{N}$, and thus, for each $i \in \{1, \dots, l\}$, $\sigma_i^{m_i}$ is a disjoint product of b -cycles. Let $\Gamma = \{j \in \Omega : \sigma_i(j) = j, \text{ for all } i \in \{1, \dots, l\}\}$. From $b \mid n$, we get $b \mid |\Gamma|$, so that Γ can be partitioned into $k = |\Gamma|/b \geq 0$ subsets Γ_j of size b , for $j \in \{1, \dots, k\}$. The set of orbits of the $\sigma_i^{m_i}$ over all $i \in \{1, \dots, l\}$ together with the sets Γ_j over all $j \in \{1, \dots, k\}$, is thus a (b, m) -block system \mathcal{B} for Ω . Now note that each σ_i commutes with $\sigma_i^{m_i}$, as well as with each σ_j , $j \neq i$. Moreover each σ_i fixes every Γ_j . Thus each σ_i stabilizes the block system \mathcal{B} . It follows that $\langle \sigma_1, \dots, \sigma_l \rangle$ is contained in the stabilizer of \mathcal{B} in S_n and thus in a suitable conjugate of $S_b \wr S_m$. \square

Corollary 5.5. *Let $n \in \mathbb{N}$ and $\sigma \in S_n$. If $b \in \mathbb{N}$, with $b \geq 2$, divides all the terms x_i in $T_\sigma = [x_1, \dots, x_k]$, then σ is contained in a conjugate of $S_b \wr S_{n/b}$.*

Proof. Split $\sigma = \sigma_1 \cdots \sigma_k$ into disjoint cycles σ_i of length x_i , for $i \in \{1, \dots, k\}$. By Lemma 5.4, $\langle \sigma_1, \dots, \sigma_l \rangle$ is contained in a conjugate of $S_b \wr S_{n/b}$. In particular $\sigma \in \langle \sigma_1, \dots, \sigma_l \rangle$ is contained in a conjugate of $S_b \wr S_{n/b}$. \square

Corollary 5.6. *Let $n \in A$ and $M = \langle \sigma \rangle \times \langle \tau \rangle \in \mathcal{M}(S_n)$. If in the canonical form of $T_\sigma = [1^2, x_1, \dots, x_k]$ every x_i is even, then $M \leq (S_2 \wr S_{n/2})^g$, for some $g \in S_n$.*

Proof. Split $\sigma = \sigma_1 \cdots \sigma_k$ into disjoint cycles σ_i of length x_i , for $i \in \{1, \dots, k\}$ and define $\sigma_{k+1} = \tau$. Note that n is necessarily even so that $b = 2 \mid n$. Now apply Lemma 5.4 to the cycles σ_i for $i \in \{1, \dots, k+1\}$ and to $b = 2$. \square

Lemma 5.7. *Let $n \in A$ and $M = \langle \sigma \rangle \times \langle \tau \rangle \in \mathcal{M}(S_n)$. If, for some $c \in \mathbb{N}$ with $c < n$, there exists a c -cut of T_σ isolating $[1^2]$, then there exists $g \in S_n$ such that $M \leq P_x^g$, where $x = \min\{c, n - c\}$.*

Proof. Let $i, j \in \Omega$ such that $\tau = (i \ j)$, $\sigma(i) = i$ and $\sigma(j) = j$. Let $[T_1 \mid T_2]$ be a c -cut of T_σ isolating $[1^2]$, with $c < n$. Since passing from c to $n - c$ does not change $x = \min\{c, n - c\}$, we can assume that $[1^2]$ is a subpartition of T_1 . Let $\mathcal{O}_1(\sigma)$ be a subset of $\mathcal{O}(\sigma)$ containing the two orbits $\{i\}$, $\{j\}$ and such that $T_1 = T_{\mathcal{O}_1(\sigma)}$. Then $O_1(\sigma) = \bigcup_{X \in \mathcal{O}_1(\sigma)} X$ has size c . We show that $\sigma, \tau \in G = \{\psi \in S_n : \psi(O_1(\sigma)) = O_1(\sigma)\}$. For σ this is a trivial consequence of the fact that $O_1(\sigma)$, by definition, is union of orbits of σ . On the other hand, since every orbit of τ , up to $\{i, j\}$, is a singleton and $O_1(\sigma) \supseteq \{i, j\}$, we have that $O_1(\sigma)$ is also a union of orbits of τ . Thus, $G = P_x^g$, for a suitable $g \in S_n$. \square

Proposition 5.8. *Let $n \in A$. Then $\gamma'(S_n) \leq g(n)$.*

Proof. If n is odd, by Propositions 5.1 and 5.3, we immediately have $\gamma'(S_n) = \gamma(S_n) \leq g(n)$. Let n be even so that $p_1 = 2$ in (5.1). Let first $\nu(n) = 1$, that is, $n = 2^\alpha$, for some $\alpha \geq 2$. By [2, Proposition 7.5],

$$\delta = \{S_2 \wr S_{2^{\alpha-1}}, P_x : 1 \leq x < 2^{\alpha-1}, x \text{ odd}\}$$

is a minimal basic set for S_n of size $g(n) = 2^{\alpha-2} + 1$. We show that δ is special checking that every $M = \langle \sigma \rangle \times \langle \tau \rangle \in \mathcal{M}(S_n)$ is contained, up to conjugacy, in a subgroup belonging to δ . Let $T_\sigma = [1^2, x_1, \dots, x_k]$ be the canonical form of T_σ as described in 3.2.1, so that for a suitable $s \in \mathbb{N}$, with $s \leq k$, x_i is even for $1 \leq i \leq s$ and x_i is odd for $s < i \leq k$. Let $m = k - s \geq 0$. If $m = 0$, then x_i is even for all $1 \leq i \leq k$ and so, by Corollary 5.6, $M \leq (S_2 \wr S_{2^{\alpha-1}})^g$, for some $g \in S_n$ and $S_2 \wr S_{2^{\alpha-1}} \in \delta$. If $m > 0$, then x_k is odd and $n/2 = 2^{\alpha-1}$ being even, we have $x_k \neq n/2$. Thus, if $x = \min\{x_k, n - x_k\}$, we have that $P_x \in \delta$. Moreover $T_\sigma = [x_k \mid 1^2, x_1, \dots, x_{k-1}]$ is a x_k -cut for T_σ isolating $[1^2]$. Then, by Lemma 5.7, we get $M \leq P_x^g$, for some $g \in S_n$.

Next let $\nu(n) = 2$, $(\alpha_1, \alpha_2) = (1, 1)$, so that $n = 2p_2$, with p_2 an odd prime. By [2, Proposition 7.6],

$$\delta = \{S_2 \wr S_{p_2}, P_x : 1 \leq x < n/2, x \text{ odd}\}$$

is a minimal basic set for S_n of size $g(n) = \frac{p_2+1}{2}$. We need only to show that any $M = \langle \sigma \rangle \times \langle \tau \rangle \in \mathcal{M}(S_n)$ is contained, up to conjugacy, in a subgroup belonging to δ . Let, as before, $T_\sigma = [1^2, x_1, \dots, x_k]$ be the canonical form of T_σ . If $m = 0$, then x_i is even for all $1 \leq i \leq k$ and so, by Corollary 5.6, $M \leq (S_2 \wr S_{p_2})^g$, for some $g \in S_n$. If $m > 0$, $n - 2 - \sum_{i=1}^s x_i$ being even, we have that $m \geq 2$ is also even. Thus T_σ admits at least two odd terms among the x_i for $1 \leq i \leq k$. Let them be x_u, x_v . Since $x_u + x_v \leq n - 2$, one of them is less than $n/2$. Calling that term x , we have $P_x \in \delta$. Moreover we have a cut for $T_\sigma = [T_1 \mid T_2]$, isolating $[1^2]$, in which $T_1 = [x]$ and T_2 is the complementary partition. Thus, by Lemma 5.7, we deduce that $M \leq P_x^g$, for some $g \in S_n$.

Finally let $\nu(n) = 2$ and $(\alpha_1, \alpha_2) \neq (1, 1)$ or $\nu(n) \geq 3$. By Proposition 5.3, we have that

$$\delta = \{P_x : 1 \leq x < n/2, \gcd(x, 2p_2) = 1\} \cup \{S_2 \wr S_{n/2}, S_{p_2} \wr S_{n/p_2}\}$$

is a basic set for S_n of size $g(n) = \frac{n}{4}(1 - \frac{1}{p_2}) + 2$. We show that δ is special. Let $M = \langle \sigma \rangle \times \langle \tau \rangle$ and $T_\sigma = [1^2, x_1, \dots, x_k]$, as above, be the canonical form of T_σ . If $m = 0$, then as in the previous cases, we get $M \leq (S_2 \wr S_{n/2})^g$, for some $g \in S_n$. Next assume $m > 0$. Then for every $i \in \{s+1, \dots, k\}$, we have x_i odd. If there exists one of those x_i with $p_2 \nmid x_i$, then we necessarily have $x_i \neq n/2$, because p_2 divides $n/2$. It follows that P_x , with $x = \min\{x_i, n - x_i\}$, belongs to δ . By Lemma 5.7, applied to the cut of T_σ with $T_1 = [x]$, we then get $M \leq P_x^g$, for some $g \in S_n$. It remains to consider the case in which $p_2 \mid x_i$, for all $i \in \{s+1, \dots, k\}$. Consider the x_i with $1 \leq i \leq s$. We cannot have all of them divisible by p_2 because this would imply $p_2 \mid n - (n - 2) = 2$, contradicting p_2 odd. Thus there exists $u \in \{1, \dots, s\}$ such that $p_2 \nmid x_u$. Pick a term x_v with $v \in \{s+1, \dots, k\}$ and consider the c -cut $T_\sigma = [x_u, x_v \mid T_2]$, where $c = x_u + x_v < n$ and T_2 is the complementary partition of $T_1 = [x_u, x_v]$. Note that the cut isolates $[1^2]$ and that $2, p_2 \nmid c$. In particular $c \neq n/2$ and thus, by Lemma 5.7, defining $x = \min\{c, n - c\}$, we have $P_x \in \delta$ and $M \leq P_x^g$, for some $g \in S_n$. □

Corollary 5.9. *Let $n \in A$. If $\gamma(S_n) = g(n)$, then $r(S_n) = \gamma'(S_n) = \gamma(S_n)$.*

Proof. It is an immediate consequence of Propositions 1 and 5.9. □

5.3. The degrees 10 and 14. We present now two interesting examples. To treat them, we need to recall some classic results.

Lemma 5.10. ([12, Theorem 13.8], [6, Theorem 4.11]) *A primitive group of degree n , which contains a permutation of type $[1^{n-m}, m]$, where $2 \leq m \leq n - 5$, contains A_n .*

Lemma 5.11. ([2, Lemma 3.5]) *Let $H \leq S_n$ be a primitive group containing an n -cycle. Then the following holds:*

- a) *If H is simply transitive or solvable, then $H \leq \text{AGL}_1(p)$ with $n = p$ a prime, or $H = S_4$ with $n = 4$.*
- b) *If H is nonsolvable and doubly transitive, then one of the following holds:*
 - i) *$H = S_n$ for some $n \geq 5$, or $H = A_n$ for some odd $n \geq 5$;*
 - ii) *$\text{PGL}_d(q) \leq H \leq \text{P}\Gamma\text{L}_d(q)$ and H acts on $n = (q^d - 1)/(q - 1)$ points or hyperplanes, where $d \geq 2$ and q is a prime power;*
 - iii) *$H = \text{PSL}_2(11)$, M_{11} or M_{23} with $n = 11, 11$ or 23 respectively.*

Lemma 5.12. ([2, Lemma 3.8]) *Let H be a group such that $\text{PSL}_d(q) \leq H \leq \text{P}\Gamma\text{L}_d(q)$, where $d \geq 2$ and q is a prime power. Then H , in its action on the $n = (q^d - 1)/(q - 1)$ points or hyperplanes, contains an $(n - 1)$ -cycle if and only if $d = 2$ and either q is a prime or $(q, H) = (4, \text{P}\Gamma\text{L}_2(4))$.*

Proposition 5.13. $\gamma(S_{10}) = \gamma'(S_{10}) = 3$ and $\gamma(S_{14}) = \gamma'(S_{14}) = 4$. Moreover, for $n \in \{10, 14\}$, no minimal basic set of S_n contains P_2 .

Proof. Let $n = 10$. By [5, Table 1], we have that $\gamma(S_{10}) = 3 = g(10)$ and thus, by Corollary 5.9, we also have $\gamma'(S_{10}) = 3$. Assume that there exists a minimal basic set of S_{10} of type $\delta = \{P_2, H, K\}$ for some H, K maximal subgroups of S_{10} and K transitive with $[10] \in K$. If $A_{10} \in \delta$, then $H = A_{10}$. Consider the types $T_1 = [1, 4, 5]$ and $T_2 = [1, 3, 6]$. They do not belong to P_2 and to A_{10} , so they must belong to K . Then $K \neq A_{10}$ contains also the type $[1^6, 4]$ and so, by Lemma 5.10, K is imprimitive. Thus $K \in \{S_2 \wr S_5, S_5 \wr S_2\}$ and so T_2 does not belong to K , a contradiction. Assume next that $A_{10} \notin \delta$ and consider the types $T_1 = [1, 9], T_2 = [3, 7]$. Since $\gcd(3, 7) = 1$, by Lemma 5.2 in [2], the only maximal subgroup of S_{10} , containing a permutation of type T_2 and different from A_{10} is P_3 . Thus $H = P_3$. Since 10 is not a prime, by Lemma 5.11, we deduce that K is 2-transitive. Moreover, since the only way to write $10 = (q^d - 1)/(q - 1)$ is $10 = 9 + 1$, we have that $K = \text{PTL}_2(9)$. On the other hand, by Lemma 5.12, since 9 is not a prime, such K cannot contain the type T_1 . Since T_1 does not belong also to P_2, P_3 , we have a contradiction.

Let now $n = 14$. We know from [2, Proposition 7.6] and from [1, Proposition 3.4] that $\gamma(A_{14}) = 4$ and that $3 \leq \gamma(S_{14}) \leq 4 = g(14)$. We first show that $\gamma(S_{14}) = 4$. Assume, by contradiction, that $\gamma(S_{14}) = 3$. Then a minimal normal covering of S_{14} must involve A_{14} as a component otherwise, by intersection, we would get a normal covering of size 3 for A_{14} contradiction $\gamma(A_{14}) = 4$. Let then $\delta = \{A_{14}, H, K\}$ be a basic set for S_{14} , with H, K maximal subgroups of S_{14} and K transitive with $[14] \in K$. By Lemma 5.10, the types $[1, 2, 11], [3, 6, 5]$ cannot belong to a primitive subgroup of S_{14} . But clearly they do not belong to either of the two imprimitive maximal subgroups of S_{14} , which are $S_2 \wr S_7$ and $S_7 \wr S_2$. So the only maximal subgroups containing them are intransitive. Since there is at most one intransitive component in δ , we deduce that $P_3 \in \delta$. Since no permutation of type $T_1 = [1, 1, 12], T_2 = [1, 4, 9]$ belongs to A_{14} and to P_3 , we deduce that $T_1, T_2 \in K$ and thus $K \neq A_{14}$ is 2-transitive and contains a 4-cycle, contradicting Lemma 5.10.

By Corollary 5.9, we immediately have $\gamma'(S_{14}) = 4$. We are left with showing that there exists no minimal basic set of S_{14} containing P_2 . By contradiction, assume that there exists a minimal basic set of S_{14} of type $\delta = \{P_2, H, K, L\}$ for some H, K, L maximal subgroups of S_{14} and L transitive with $[14] \in L$. If $A_{14} \in \delta$, then let $H = A_{14}$ and note that in δ , other than P_2 , there is at most one intransitive component. Consider the types $T_1 = [1, 3, 10], T_2 = [3, 5, 6]$ and $T_3 = [1, 5, 8]$. They do not belong to P_2 and to A_{14} and, by Lemma 5.10, they do not belong to primitive subgroups. On the other hand they also do not belong to $S_2 \wr S_7$ and $S_7 \wr S_2$. Thus they require an intransitive component. But there exists no intransitive maximal subgroup of S_{14} containing all the T_i , for $i \in \{1, 2, 3\}$. Assume next that $A_{14} \notin \delta$ and consider the types $T_1 = [1, 13], T_2 = [3, 11], T_3 = [5, 9], T_4 = [4, 10]$. Since $\gcd(3, 11) = \gcd(5, 9) = 1$, by Lemma 5.2 in [2], the only maximal subgroup

of S_{14} , containing a permutation of type T_2 and different from A_{14} is P_3 . So $P_3 \in \delta$. Similarly, dealing with T_3 , we get that $P_5 \in \delta$. Thus, we have $\delta = \{P_2, P_3, P_5, L\}$ and necessarily $T_1 \in L$. Thus, by Lemma 5.11, we get $L = \text{PGL}_2(13)$. But then $5 \nmid |L|$ and so no component of δ contains T_4 because a permutation of type T_4 has order 20. \square

The above result and Proposition 5.1 inspire the following

Group-theoretic Question 2. *Do there exist infinitely many even $n \in \mathbb{N}$, such that no minimal basic set of S_n admits P_2 as a component?*

5.4. The h bound. In this section we produce a second collection of upper bounds for $\gamma'(S_n)$, using the special basic set δ_1 below, communicated to the first author by Attila Maróti [9]¹, and a further basic set δ_2 , which turns out to be particularly useful when n is odd. These new bounds improve the $g(n)$ bound only when $\nu(n)$ is large and n is odd. To appreciate the order of magnitude of the new bounds, we recall a number theoretical result from [2]. For f, g real functions defined over an upper unbounded domain, write $f \sim g$ if $\lim_{x \rightarrow +\infty} \frac{f(x)}{g(x)} = 1$. Let $n \in \mathbb{N}$ and let $0 \leq x < y \leq n$, with $x, y \in \mathbb{R}$. For any interval I with extremes x and y , define

$$\phi(I; n) = |\{i \in \mathbb{N} : i \in I, (i, n) = 1\}|.$$

By [2, Lemma 2.3], we then have that if $y - x \sim cn$ for some $c > 0$, then $\phi(I; n) \sim c\phi(n)$.

Proposition 5.14. *Let $n \in \mathbb{N}, n \geq 6$, not a prime. Then:*

i) (Maróti)

$$\delta_1 = \{P_x : 1 \leq x \leq n/3\} \cup \{P_x : n/3 < x < n/2, \gcd(x, n) = 1\} \cup$$

$$\{S_{p_i} \wr S_{n/p_i} : i \in \{1, \dots, \nu(n)\}\}$$

is a special basic set of size

$$\lfloor n/3 \rfloor + \nu(n) + \phi((n/3, n/2); n) \sim n/3 + \nu(n) + \phi(n)/6;$$

ii) *if n is odd, then*

$$\delta_2 = \{P_x : 1 \leq x \leq n/4\} \cup \{P_x : n/4 < x < n/2, \gcd(x, n) = 1\} \cup$$

$$\{S_{p_i} \wr S_{n/p_i} : i \in \{1, \dots, \nu(n)\}\} \cup \{A_n\}$$

is a special basic set of size

$$\lfloor n/4 \rfloor + \nu(n) + \phi((n/4, n/2); n) + 1 \sim n/4 + \nu(n) + \phi(n)/4.$$

¹Maróti's motivation was his proof that there are infinitely many n for which $\gamma(S_n) < g(n)$, refuting [5, Conjecture 1] which states that, for $\nu(n) \geq 2$ and $n \neq p_1 p_2$, $\gamma(S_n) = g(n)$.

Proof. First of all, note that the condition n not a prime guarantees that, for every $i \in \{1, \dots, \nu(n)\}$, $S_{p_i} \wr S_{n/p_i} \in \mathcal{W}$.

i) Since $n \geq 6$, we have that $P_2 \in \delta_1$ and thus, by Corollary B, it is enough to show that δ_1 is a basic set. By Corollary 5.5, the n -cycles belong, up to conjugacy, to $S_{p_1} \wr S_{n/p_1} \in \delta_1$. Consider the types $T_x = [x, n-x]$, with $1 \leq x \leq n/2$. If $\gcd(x, n) = 1$, then $x \neq n/2$ and T_x belong to $P_x \in \delta$; if $\gcd(x, n) \neq 1$, then there exists p_i such that $p_i \mid x$ and so, by Corollary 5.5, T_x belongs to $S_{p_i} \wr S_{n/p_i}$. Finally let $T = [x_1, \dots, x_k]$, with $k \geq 3$. Then at least one term is less or equal to $n/3$ and thus T belongs to P_x for some $1 \leq x \leq n/3$.

ii) Since $n \geq 9$, we have that $P_2 \in \delta_2$ and thus, by Corollary B, it is enough to show that δ_2 is a basic set. For the types $[n]$ and $T_x = [x, n-x]$, with $1 \leq x \leq n/2$, we argue as in i). If $T = [x_1, x_2, x_3]$, then, being n odd, T belongs to A_n . Finally if $T = [x_1, \dots, x_k]$, with $k \geq 4$, then at least one term is less than or equal to $n/4$, and thus T belongs to P_x for some $1 \leq x \leq n/4$. □

Definition 5.15. Define the function $h : A \rightarrow \mathbb{N}$ by

$$h(n) = \begin{cases} \lfloor n/3 \rfloor + \nu(n) + \phi((n/3, n/2); n) & \text{if } n \text{ is even} \\ \lfloor n/4 \rfloor + \nu(n) + \phi((n/4, n/2); n) + 1 & \text{if } n \text{ is odd} \end{cases}$$

Corollary 5.16. Let $n \in A$. Then $\gamma'(S_n) \leq h(n)$.

Proof. If $n \geq 6$ and n is not a prime, then the result follows from Proposition 5.14. If $n = 4$, note that $h(4) = 2 = \gamma'(S_4)$. If $n = p$ is a prime we have that $h(p) = 2 + \frac{p-1}{2} > \gamma'(S_p) = \frac{p-1}{2}$. □

Depending on n , we may have, in principle, $h(n) > g(n)$ or $g(n) > h(n)$ and thus, correspondingly, either the bound expressed by Proposition 5.8 or that expressed by Corollary 5.16 is more strict. The next proposition shows that the bound given by Proposition 5.8 is always preferable when n is even. Note also that $g(4) = h(4)$.

Proposition 5.17. Let $n \in \mathbb{N}, n \geq 5$. If n is even, then $g(n) < h(n)$. If n is odd, then there exists infinitely many n such that $h(n) < g(n)$.

Proof. Let n be even. If $n \leq 22$, direct computation shows that $g(n) < h(n)$. If $n \geq 24$, we have $g(n) \leq \frac{n}{4}(1 - \frac{1}{p_2}) + 2 < n/4 + 2 \leq n/3 \leq h(n)$.

To construct an infinite family of natural numbers n such that $h(n) < g(n)$, we proceed as follows. Define $n_k = p_1 p_2 \cdots p_k$ to be the product of $k \geq 3$ consecutive odd primes. We have $\lim_{k \rightarrow +\infty} \frac{\phi(n_k)}{n_k} = 0$ as well as $\lim_{k \rightarrow +\infty} \frac{\nu(n_k)}{n_k} = 0$ and hence $\lim_{k \rightarrow +\infty} \frac{h(n_k)}{n_k} = \frac{1}{4}$. On the other hand, we have $\lim_{k \rightarrow +\infty} \frac{g(n_k)}{n_k} = \frac{1}{2}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$. Choose now the primes p_1, p_2 such that $(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) > \frac{1}{2}$. With this choice of p_1, p_2 , we get $\lim_{k \rightarrow +\infty} \frac{g(n_k) - h(n_k)}{n_k} > 0$ and thus $h(n_k) < g(n_k)$ for an infinite number of n_k . □

5.5. The even degree case. We focus now on the case n even, trying to shed light on the Group-theoretic Question 2. To appreciate what we are going to show, note that the canonical basic set δ_C in (5.3) does not contain P_2 .

Proposition 5.18. *Let $n \in A$ be even. Then the set*

$$\delta_E = \{P_x : 1 \leq x < n/2, 2 \mid x\} \cup \{S_{n/2} \wr S_2\} \cup \{A_n\}$$

is a special basic set of size $|\delta_E| = \lceil \frac{n+4}{4} \rceil$. Moreover, $g(n) \leq |\delta_E|$ with equality if and only if $n = 2^\alpha$, for some $\alpha \in \mathbb{N}$ with $\alpha \geq 2$, or $n = 4q$, for some prime q .

Proof. Let n be even. We show that δ_E is a special basic set for S_n . Since $P_2 \in \delta_E$, by Proposition 1, it is enough to show that δ_E is a basic set, that is, all the types of S_n appear in some component of δ_E . By Corollary 5.5, the type $[n]$ belongs to $S_{n/2} \wr S_2$. The types with an even number of parts belong instead to A_n . Let $T = [x_1, \dots, x_k]$ be a type with an odd number $k \in \mathbb{N}$ of parts. Then, there exists an even term x_i . If $x_i \neq n/2$, then consider $x = \min\{x_i, n - x_i\} < n/2$ and note that $T \in P_x$. If instead the only even term is equal to $n/2$, then $T \in S_{n/2} \wr S_2$. The size of δ_E is clear counting the even numbers in $[1, n/2) \cap \mathbb{N}$.

We show that $|\delta_E| \leq g(n)$, taking into account the cases of the definition (5.2) of $g(n)$. Let first $4 \mid n$, so that $|\delta_E| = \frac{n}{4} + 1$. If $n = 2^\alpha$ for some $\alpha \in \mathbb{N}$ with $\alpha \geq 2$ we have $g(n) = \frac{n}{4} + 1$. If $\nu(n) \geq 2$ and $n = 2^{\alpha_1} \cdots p_{\nu(n)}^{\alpha_{\nu(n)}}$, for some $\alpha_1 \geq 2$ and $\alpha_i \geq 1$ for $i \in \{1, \dots, \nu(n)\}$, then $g(n) = \frac{n}{4}(1 - \frac{1}{p_2}) + 2 \leq \frac{n}{4} + 1$. Moreover, it is immediately checked that $g(n) = \frac{n}{4} + 1$ holds only if $n = 4p_2$. Consider next the case $4 \nmid n$ so that $|\delta_E| = \frac{n+6}{4}$. Since $n \geq 4$, we have $\nu(n) \geq 2$ and $n = 2p_2^{\alpha_2} \cdots p_{\nu(n)}^{\alpha_{\nu(n)}}$, with $\alpha_i \geq 1$ for $i \in \{1, \dots, \nu(n)\}$. If $\nu(n) = 2$ and $\alpha_2 = 1$, we have $n = 2p_2$ and $g(n) = \frac{n+2}{4} = |\delta_E| - 1 < |\delta_E|$. If instead $\alpha_2 \geq 2$ or $\nu(n) \geq 3$, we have that $\frac{n}{p_2} > 2$ and thus $g(n) = \frac{n}{4}(1 - \frac{1}{p_2}) + 2 < \frac{n+6}{4}$. \square

Corollary 5.19. *Let $n \in A$ be even of the type $n = 2^\alpha$, for some $\alpha \in \mathbb{N}$ with $\alpha \geq 2$, or $n = 4q$ for some prime q . If $\gamma(S_n) = g(n)$, then there exists a minimal basic set of S_n containing P_2 as a component.*

Proof. By $\gamma(S_n) = g(n)$, we get that the basic set δ_E in Proposition 5.18 is minimal. Moreover, by definition, $P_2 \in \delta_E$. \square

Recall that we do not know any infinite family of even n such that $\gamma(S_n) = g(n)$. Thus the above result does not imply the existence of infinitely many even n such that P_2 appears as a component in some minimal basic set. Note that Proposition 5.18 implies that Conjecture 3 in [5], stating that for each minimal basic set of S_n , with $\nu(n) \geq 2$, consisting of maximal components, the subset of intransitive components is given by $\{P_x \in \mathcal{P} : \gcd(x, p_1 p_2) = 1\}$, is generally false for n even. Indeed we have $\gamma(S_{12}) = 4 = g(12)$ and in the intransitive components $P_x \in \delta_E$, x is even.

We close this section observing, as a further consequence of Proposition 5.18, that no kind of uniqueness seems possible for the minimal special basic sets in the even case. For instance the three sets of subgroups of S_8 given by

$$\delta_E = \{P_2, A_8, S_4 \wr S_2\}, \quad \delta_C = \{P_1, P_3, S_4 \wr S_2\}, \quad \delta = \{P_1, A_8, S_2 \wr S_4\}$$

are all minimal special basic sets for S_8 . This follows from $\gamma(S_8) = 3 = g(8)$, using Corollary 5.9 for δ_C and using Proposition 5.18 for δ_E . For the set δ the check is easily carried on by the usual arguments.

6. LINEAR BOUNDS FOR $r(S_n)$ AND $\gamma'(S_n)$

In this last section we derive for the parameter $r(S_n)$ and $\gamma'(S_n)$, the same linear bounds (1.1) known for $\gamma(S_n)$.

Proposition 6.1. *Let $n \in \mathbb{N}, n \geq 3$. Then there exists a positive constant k such that $kn \leq r(S_n) \leq \gamma'(S_n) \leq 2n/3$.*

Proof. If $n = 3$, we use (4.1) and $k \leq 2/3$. Let $n \geq 4$. By Proposition 1 and Proposition 5.8, we know that

$$\gamma(S_n) \leq r(S_n) \leq \gamma'(S_n) \leq g(n).$$

Since, by [4, Theorem 1.1], $\gamma(S_n) \geq kn$, we immediately derive the lower bound $kn \leq r(S_n) \leq \gamma'(S_n)$. To deal with the upper bound, consider the function $g(n)$. Since the function $f(x) = 1 - 1/x$ is increasing for $x > 0$, we have that $g(n) < n/2 + 2$, and $g(n)$ being an integer says $g(n) \leq \frac{n+3}{2}$. If $n \geq 9$, we note that $\frac{n+3}{2} \leq 2n/3$. The cases $4 \leq n \leq 8$ are all included in [5, Table 1] and realise $\gamma(S_n) = g(n)$, so that by Corollary 5.9 and [4, Theorem 1.1], we also have $\gamma'(S_n) = \gamma(S_n) \leq 2n/3$. \square

In conclusion we note that the constant k relies on certain number theoretic results (see [3]) and that the known value of k is unrealistically small because of the many approximations needed first to obtain and next to apply those results. For instance, we know that for $n \geq 792,000$ even, $k = 0.025$ works ([4, Remark 6.5.]). We still do not know optimum values for the constant k .

7. ACKNOWLEDGMENTS

The authors wish to thank Attila Maróti for his permission to use his personal communication, which led to Section 5.4. The first author is supported by GN-SAGA (INdAM).

REFERENCES

- [1] R. Brandl, D. Bubboloni, and I. Hupp, Polynomials with roots mod p for all primes p , *J. Group Theory* 4: 233–239, 2001.
- [2] D. Bubboloni and C. Praeger, Normal coverings of finite symmetric and alternating groups, *J. Combinatorial Theory, Ser. A*, 118: 2000–2024, 2011.

- [3] D. Bubboloni, F. Luca and P. Spiga, Compositions of n satisfying some coprimality conditions, *J. Number Theory*, 132: 2922-2946, 2012.
- [4] D. Bubboloni, C. E. Praeger and P. Spiga, Normal coverings and pairwise generation of finite alternating and symmetric groups, *J. Algebra*, 390: 199-215, 2013 .
- [5] D. Bubboloni, C. Praeger and P. Spiga, Conjectures on the normal covering number of the finite symmetric and alternating groups, *Int. J. Group Theory*, vol. 3 no. 2: 57-75, 2014.
- [6] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts 45, Cambridge University Press, Cambridge, 1999.
- [7] K. S. Kedlaya, A construction of polynomials with squarefree discriminants, *Proc. AMS* 140: (no. 9): 3025-3033, 2012.
- [8] T. Kondo, Algebraic number fields with the discriminant equal to that of a quadratic number field, *J. Math. Soc. Japan* 47: 31-36, 1995.
- [9] A. Maróti, Personal communication, 2013.
- [10] D. Rabayev and J. Sonn, On Galois realizations of the 2-coverable symmetric and alternating groups, *Comm. Alg.* 42, no. 1: 253-258, 2014.
- [11] Jack Sonn, Polynomials with roots in \mathbb{Q}_p for all p , *Proc. Amer. Math Soc.* 136, no. 6: 1955–1960, 2008.
- [12] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York-London, 1964.

DEPARTMENT OF ECONOMICS AND MANAGEMENT, UNIVERSITY OF FIRENZE, VIA DELLE
PANDETTE 9, 50127 FIRENZE, ITALY

E-mail address: `daniela.bubboloni@unifi.it`

DEPARTMENT OF MATHEMATICS, TECHNION — ISRAEL INSTITUTE OF TECHNOLOGY, HAIFA,
32000, ISRAEL

E-mail address: `sonn@math.technion.ac.il`